CB-BEITRAG

Jens-Christof Niemeyer, RA

Step-by-step: Durchsuchung von Computern, Smartphones und sonstigen Datenspeichern

Die Zulässigkeit des arbeitgeberseitigen Zugriffs auf die E-Mail-Konten seiner Mitarbeiter ist im Schrifttum umfassend behandelt worden. Dem Thema wird bereits das Zeug zum „Klassiker" zugeschrieben (*Lensdorf/Born*, CR 2013, 30). Über die Frage, wann nicht nur auf E-Mail-Konten, sondern auch auf Festplatten, Smartphones und sonstige Datenspeicher zugegriffen werden darf, herrscht in der IT-Forensik Unsicherheit. Nicht selten wird dies bei Durchsuchungen anlässlich des Verdachts einer Straftat des Mitarbeiters zum Nachteil des Arbeitgebers von Bedeutung sein. In diesem Kontext relevant werden können: Umstände, die in der Person des jeweiligen Mitarbeiters liegen, die Eigentumsverhältnisse am Untersuchungsgegenstand (Stichwort *Bring your own Device*, kurz *BYOD*), der konkrete Untersuchungsbereich und die Gestattung der privaten Nutzung. Im Folgenden wird eine systematische Orientierungshilfe für die Praxis vorgelegt. Soweit die Zulässigkeit nicht bejaht wird, sensibilisiert der Beitrag für die Besonderheiten des jeweiligen Einzelfalls.

1 In der Person des Mitarbeiters liegende Umstände

Falls der Untersuchungsgegenstand von einem Berufsgeheimnisträger oder einem anderweitig mit Sonderstatusrechten versehenen Arbeitnehmer genutzt wird, verbietet sich die schematische Bejahung der Zulässigkeit der Durchsuchung. Dies gilt insbes. dann, wenn die Maßnahme unter Hinzuziehung eines externen Dienstleisters vollzogen werden soll.

Geheimnisträger, die ihr dienstlich erlangtes Wissen nicht an Dritte weitergeben dürfen, sind gem. § 203 StGB Angehörige der Heilberufe, deren Berufsausübung an eine staatlich geregelte Ausbildung anknüpft (Heilpraktiker sind also nicht erfasst), insbes. Ärzte, Zahnärzte, Tierärzte, Apotheker, Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung, Rechtspflege- und Wirtschaftsberatungsberufe, also Rechts- und Patentanwälte, Notare, Verteidiger, Wirtschafts- und vereidigte Buchprüfer, Steuerberater und -bevollmächtigte sowie Organe oder Mitglieder eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft sowie andere Mitglieder einer Anwaltskammer (§ 203 Abs. 3 S. 1 StGB), Ehe-, Familien-, Erziehungs-, Jugendberater und Berater für Suchtfragen, Mitglieder oder Beauftragte einer anerkannten Beratungsstelle i. S. d. Schwangerschaftskonfliktgesetzes, staatlich anerkannte Sozialarbeiter und Sozialpädagogen, Angehörige von Unternehmen der privaten Kranken-, Unfall- und Lebensversicherung sowie der privatärztlichen, steuerberaterlichen und anwaltlichen Verrechnungsstellen.

Berufsmäßig tätige Gehilfen sind den Geheimnisträgern gleichgestellt. Zu den vom Straftatbestand des § 203 StGB erfassten Personengruppen gehören ferner Amtsträger, für den öffentlichen Dienst besonders Verpflichtete (innerhalb einer Behörde sowie gegenüber Aufsichtsbehörden i. d. R. nicht problematisch; *Fischer*, StGB, 2010, § 203 StGB, Rn. 41), Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen (zum Themenkomplex *Betriebsrats-PC* siehe LAG Düsseldorf, 7.3.2012 – 4 TaBV 87/11; LAG Berlin-Brandenburg, 4.3.2011 – 10 TaBV 1984/10), Mitglieder oder Hilfskräfte von Ausschüssen, die für ein Gesetzgebungsorgan des Bundes oder eines Landes tätig sind, öffentlich bestellte Sachverständige, Personen, die im Rahmen wissenschaftlicher Forschungsvorhaben auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht förmlich verpflichtet worden sind, und Datenschutzbeauftragte.

Mit Blick auf Zeugnisverweigerungsrecht und Informantenschutz ist auch bei Journalisten Vorsicht geboten. Die Zulässigkeit einer Durchsuchung ist Frage des Einzelfalls, da die sog. *innere Pressefreiheit* keinen vorbehaltlosen Geheimnisschutz angestellter Journalisten gegenüber dem Arbeitgeber begründet (*Elschner*, in: *Hoeren/Sieber*, Handbuch Multimedia-Recht, 33. EL 2013, Kap. 22.1, Rn. 180). Dasselbe sollte bei den weiteren in § 53 StPO genannten Berufsgruppen, also insbes. Geistlichen und Parlamentariern, beachtet werden. Geräte und Kommunikationsverhalten des Betriebsrats haben in aller Regel ebenfalls außer Betracht zu bleiben (*Elschner*, in: *Hoeren/Sieber*, Handbuch Multimedia-Recht, dto., Kap. 22.1, Rn. 194 ff.).

Die in einer solchen Mitarbeiterkonstellation angezeigten Veranlassungen und Handlungsoptionen sind nicht Gegenstand dieses Beitrags (denkbar ist ggf. die Einschaltung der Strafverfolgungsbehörden im Interesse der Veranlassung von Zwangsmaßnahmen nach Maßgabe des 8. Abschnitts des 1. Buchs der StPO, später mag der Arbeitgeber Akteneinsicht nehmen).

Weitere Besonderheiten sind zu beachten, wenn der Mitarbeiter Beamter, Richter oder Soldat ist. Bei Beamten ist vor einer Durchsuchungsmaßnahme ein Disziplinarverfahren einzuleiten, in dessen Rahmen die Durchsuchung gem. § 27 Abs. 1 BDG (Bundesdisziplinargesetz) verwaltungsrichterlich angeordnet werden muss (*Herrmann/Soiné*, NJW 2011, 2922). Erforderlich ist der dringende Verdacht eines so schwer

wiegenden Dienstvergehens, das eine Entfernung aus dem Dienst, die Aberkennung des Ruhegehalts oder wenigstens eine Zurückstufung rechtfertigt. Eine das spätere Disziplinarverfahren vorbereitende Durchsuchung kann vor dessen Einleitung nicht auf andere gesetzliche Bestimmungen gestützt werden (*BVerwG*, 31.3.2011 – 2 A 11.08).

2 Verfügungsbefugnis über den Untersuchungsgegenstand

Soweit die unmittelbare Durchsuchung nicht an Umständen scheitert, die in der Person des Mitarbeiters liegen, ist der Frage nachzugehen, wem der Untersuchungsgegenstand gehört bzw. wem die Verfügungsbefugnis zusteht.
In einer BYOD-Konstellation, wenn das Gerät also aus der Sphäre des Mitarbeiters stammt, dürfen regelmäßig nur Daten ausgelesen werden, die sich in einem ausdrücklich für Unternehmensdaten vorgesehenen Ordner befinden (*Arning/Moos/Becker*, CR 2012, 592, 594), vorausgesetzt, hierzu existiert eine vertragliche Regelung. Anderenfalls wäre eine freiwillige, widerrufliche Einwilligung erforderlich, die entweder auf die konkrete Maßnahme bezogen ist oder im Rahmen einer – schon deshalb empfehlenswerten – BYOD-Nutzungsvereinbarung erteilt wurde (zur Tauglichkeit solcher Einwilligungen siehe *Conrad/Schneider*, ZD 2011, 153, 159).

3 Durchsuchung von Smartphones und Festplatten des Arbeitgebers

Meist wird ein der Verfügungsgewalt des Arbeitgebers unterfallendes Gerät zu untersuchen sein, etwa der Arbeitsplatzrechner des Mitarbeiters, ein Diensthandy oder ein Notebook.
Die beabsichtigte Durchsuchungsmaßnahme darf in dieser Konstellation ohne Weiteres vorgenommen werden, wenn das Gerät ausschließlich dienstlich genutzt wird. Der Arbeitgeber, dessen bloßer Handlungsgehilfe der Mitarbeiter ist, hat umfassende Kontrollbefugnisse und kann auch Kenntnis vom Inhalt der Dateien nehmen. Auf Arbeitsmitteln gespeicherte Daten unterfallen regelmäßig nicht dem Schutz der Intim- oder Privatsphäre, da Arbeitnehmer mit der Kenntnisnahme dieser Daten durch den Arbeitgeber stets rechnen müssen (*Schmidt*, Erfurter Kommentar zum Arbeitsrecht, 2012, Art. 2, Rn. 46a, 97 ff.; *Braun*, juris-PK Internetrecht, 2011, Kap. 7, Rn. 155).
Grundsätzlich darf auf elektronische Akten und Dokumente mit dienstlichem Charakter zugegriffen werden (*Schuster*, ZIS 2010, 68 ff.). Für den Fall, dass man im Verlaufe der Durchsuchung auf eine private Datei stößt, etwa weil der Dateiname dies indiziert oder sich wider Erwarten ein offensichtlich privater Ordner auf dem Gerät befindet, wird vertreten, dass der Inhalt nicht angesehen werden darf (*Braun*, juris-PK Internetrecht, 2011, Kap. 7, Rn. 101). Sollte die Untersuchung verschlüsselte Daten zutage bringen, sollten weitere Maßnahmen mit Blick auf § 202a StGB zurückgestellt werden.

4 Durchsuchung von Smartphones und Festplatten bei erlaubter oder geduldeter Privatnutzung

Selbst wenn dem betreffenden Mitarbeiter die private Nutzung des Untersuchungsgegenstands gestattet ist, ist eine Vorgehensweise wie unter Step 3 dargestellt nicht per se bedenklich. Entscheidend ist eine strikte und nachvollziehbare Trennung dienstlicher und privater Daten, da hinsichtlich der privaten Daten kein Kontrollrecht besteht. Innehalten ist daher angezeigt, wenn dienstliche und private Daten sich nur schwer unterscheiden lassen.
Mit Blick auf strengere Auffassungen und etwaige Bußgeldsanktionen könnte – Prinzip des sichersten Wegs – auch erwogen werden, eine Durchsuchung nur im Falle des Verdachts einer Straftat des Mitarbeiters gegen den Arbeitgeber vorzunehmen. Jedenfalls bei einer eingeschränkten Vertraulichkeit der Privatnutzung muss der Mitarbeiter damit rechnen, dass Spuren, die er durch die Nutzung von Ressourcen des Arbeitgebers hinterlässt, in einem Prozess gegen ihn verwendet werden (LAG Hamm, 10.7.2012 – 14 Sa 1711/10).
§ 32 Abs. 1 S. 2 BDSG gestattet die Erhebung personenbezogener Daten des Arbeitnehmers zur Aufklärung einer Straftat. Erforderlich sind tatsächliche Anhaltspunkte, die sich gegen einen Beschäftigten oder einen abgrenzbaren Kreis von Beschäftigten richten, und eine Dokumentation, also das elektronische oder schriftliche und reproduzierbare Festhalten der Umstände, die den Verdacht und die Datenerhebung rechtfertigen (*Lembke*, in: *Henssler/Willemsen/Kalb*, Arbeitsrecht, 5. Aufl. 2012, § 32 BDSG, Rn. 17 f.; *Greening/Weigl*, CR 2012, 787, 792). Hinzu kommt das Erfordernis der Abwägung der Individualinteressen des Arbeitnehmers mit denen des Arbeitgebers (Problemaufriss und widerstreitende Positionen bei *Fülbier/Splittgerber*, NJW 2012, 1995, 1997).
Auch in dieser Konstellation vermag eine freiwillige, widerrufliche Einwilligung des Mitarbeiters über die Hürde zu helfen. Zu bedenken ist, dass eine solche Einwilligung zwar als zulässig angesehen werden kann, wenn sie schon bei Begründung des Arbeitsverhältnisses erteilt wurde. Bei im laufenden Arbeitsverhältnis erteilten Einwilligungen dagegen wird die Freiwilligkeit oft in Frage gestellt (siehe nur *Taeger*, in: *Taeger/Gabel*, BDSG, 2010, § 4a, Rn. 58 ff.).

5 Untersuchung des E-Mail-Kontos

Soll die Durchsuchungsmaßnahme sich (auch) auf E-Mails des Mitarbeiters erstrecken, ist ebenfalls die Frage der Gestattung privater Nutzung zu stellen (zu E-Mail-Kontrollen sowie Handlungsempfehlungen zur Regelung der Privatnutzung: *Wybitul*, ZD 2011, 69).
Wenn die private Internetnutzung verboten ist und dieses Verbot auch durchgesetzt wird, dann werden Kontrollmaßnahmen als zulässig angesehen (siehe nur *Rath/Karner*, K&R 2010, 469, 470). Die Prüfung darf sich auch auf die Inhalte von E-Mails beziehen, solange die betreffende Nachricht nicht an eine betriebliche Interessenvertretung, den Betriebsarzt bzw. eine betriebliche Beschwerde- oder Whistleblower-Stelle gerichtet (*Seifert*, in: *Simitis*, 7. Aufl. 2011, § 32 Rn. 91) oder – wider Erwarten – ersichtlich privater Natur ist. Ebenfalls gestattet sind regelmäßige Kontrollen, deren alleiniger Zweck die Prüfung der Einhaltung des Verbots der Privatnutzung ist.

6 Untersuchung des E-Mail-Kontos bei gestatteter oder geduldeter Privatnutzung

Im Falle einer Gestattung oder Duldung der privaten Internetnutzung ist eine inhaltliche Kontrolle der Inhalte von E-Mails, Verbindungsdaten und aufgerufenen Internetseiten nach bisher herrschender

Meinung grundsätzlich unzulässig, da der Arbeitgeber dann als Diensteanbieter i. S. d. § 88 TKG angesehen wird und das Fernmeldegeheimnis zu wahren hat (siehe nur: *Schumacher*, in: *Besgen/Prinz*, Handbuch Internet. Arbeitsrecht, 2013, S. 53). Zum Inhalt des geschützten Telekommunikationsvorgangs gehört schon die Betreffzeile einer E-Mail (*Munz*, in: *Taeger/Gabel*, BDSG, 2010, § 88 TKG, Rn. 8). Normwidriges Verhalten kann als Verletzung des Fernmeldegeheimnisses (§ 206 StGB) oder nach den Strafvorschriften des BDSG (§ 44 i. V. m. § 43 Abs. 2 BDSG) strafbar sein.

Bei der Bewertung einer Durchsuchungsmaßnahme ist die zeitliche Geltung des Fernmeldegeheimnisses in den Blick zu nehmen. Dem BVerfG zufolge ist lediglich der laufende Telekommunikationsvorgang geschützt (BVerfGE 120, 274). Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten dagegen werden „nur" durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und ggf. durch die Unverletzlichkeit der Wohnung geschützt (BVerfGE 115, 166).

Auch das Transferprotokoll kann bedeutsam werden: Während beim POP3-Verfahren eine klassische Vermittlung vom Sender an den Empfänger stattfindet, werden E-Mails im IMAP-System zentral auf dem Server vorgehalten und verwaltet.

Einzig taugliche Vorgehensweise kann derzeit sein, jedenfalls ungelesene Nachrichten im Posteingang bei Kontrollen unberücksichtigt zu lassen, da deren Gelangen in den Herrschaftsbereich des Mitarbeiters fraglich ist (*Braun* fordert sogar eine weitergehende Aktivität, etwa ein Verschieben der betreffenden Nachricht aus dem Posteingang, juris-PK Internetrecht, 2011, Kap. 7, Rn. 146). Eine etwaige Vorab-Einwillligung des Mitarbeiters in die Kontrolle aller E-Mails kommt als „Gegenmittel" nicht in Betracht, da das Fernmeldegeheimnis auch die Kommunikationspartner des Mitarbeiters schützt.

Was als Duldung der Privatnutzung anzusehen ist, kann nur anhand der jeweiligen Einzelfallumstände beurteilt werden. Aus der vorbehaltlosen Bereitstellung eines unbeschränkten Internetzugangs allein lässt sich noch keine Gestattung ableiten. Auch vor der Annahme einer betrieblichen Übung ist stets zu prüfen, ob eine bestimmte Verhaltensweise dergestalt wiederholt wurde, dass der Arbeitnehmer schließen durfte, die Privatnutzung sei ihm auf Dauer gestattet. Zur weiteren Orientierung können die von *Elschner* zur konkludenten Erlaubnis entwickelten Kriterien herangezogen werden (in: *Hoeren/Sieber*, Handbuch Multimedia-Recht, 33. EL 2013, Kap. 22.1, Rn. 41 ff.). Zu denken ist etwa an die vorbehaltlose Bereitstellung privater E-Mail-Accounts oder die systemweite Installation vordefinierter Bookmarks zu Websites, die nicht in Bezug zur Arbeitsleistung stehen.

7 Jüngere Rechtsprechung: Arbeitgeber ≠ Diensteanbieter

Anders lägen die Dinge, wenn die in den Entscheidungen des LAG Niedersachen (31.5.2010 – 12 Sa 875/09) und des LAG Berlin-Brandenburg (16.2.2011 – 4 Sa 2132/10, BB 2011, 2298 m. BB-Komm. *Mückenberger/Müller*) hervortretende Rechtsauffassung sich verfestigen oder kodifiziert würde. Den Entscheidungen zufolge sind Arbeitgeber allein wegen der Gestattung der privaten Nutzung des dienstlichen E-Mail-Accounts nicht als Diensteanbieter anzusehen, sodass das Fernmeldegeheimnis nicht gilt. Es soll jedoch nicht unerwähnt bleiben, dass die jüngere Entscheidung eine erkrankte Mitarbeiterin betraf, die eine bereits eingerichtete Stellvertretungsregelung deaktiviert hatte. Das LAG Niedersachsen hatte – trotz Gestattung der Privatnutzung des Arbeitsplatzrechners – nach entsprechender Interessenabwägung zumindest keine durchgreifenden Bedenken gegen den Zugriff auf E-Mails, die vom Mitarbeiter auf dem Computer bzw. zentralen System belassen wurden.

8 Gestaltungsmöglichkeiten – §§ 130, 9 OWiG lassen grüßen

Wenn ein Verbot der privaten Nutzung betrieblicher Ressourcen nicht gewollt (moderne Unternehmenskultur) oder nur schwer durchsetzbar (Verführungen des Dienst-Tablets) ist, ist es an der Zeit für Nutzungsvereinbarungen (individuell oder per Betriebsvereinbarung).

Minimaler Regelungsinhalt ist für die Internetnutzung das Verbot jeglicher illegaler Kommunikation im Verbund mit der widerruflichen Erlaubnis privater Nutzung des E-Mail-Kontos unter den Bedingungen der Kennzeichnung privater Nachrichten und des Einverständnisses mit Kontrollen, deren Anlässe und Umstände offengelegt werden.

Im Interesse einer strikteren Trennung sollte die Beratungspraxis die drastische Beschränkung der Nutzung des dienstlichen E-Mail-Kontos bei gleichzeitigem Verweis auf Webmailer oder zusätzliche private Konten (name-privat@firma.de) forcieren.

Einen Schritt weiter geht, wer sich auch der Aufgabe stellt, auch BYOD-Konstellationen zu regeln. Pragmatisch formulieren etwa *Conrad/Schneider* die These, es sei besser, private Geräte in kontrollierbarem Umfang zuzulassen als unkontrolliertem, heimlichen Wildwuchs Vorschub zu leisten (ZD 2011, 153, 159). Einen Katalog der Mindestanforderungen an eine BYOD-Nutzungsvereinbarung haben *Arning/Moos/Becker* vorgelegt (CR 2012, 592).

Fazit

Der Schutz des Privatgeheimnisses und der Privatsphäre strahlt auf Computerdurchsuchungen aus. Der Wunsch nach Rechtssicherheit bzw. klaren Vorgaben zu E-Mail-Kontrollen besteht unverändert fort. Mit Blick auf BYOD-Konstellationen zeigt sich, dass demjenigen ein verlässlicher Handlungsspielraum eröffnet ist, der diese durch Nutzungsvereinbarungen verbindlich und interessengerecht regelt. Compliance-Erwägungen legen entsprechende Regelung auch für die Internet- und E-Mail-Nutzung nahe.

AUTOR

Jens-Christof Niemeyer, *RA, ist Einzelanwalt in Spenge. Die von Internet und Informationstechnologie aufgeworfenen Rechtsfragen gehören zu seinen Beratungsschwerpunkten.*